BEKO 300TR

Security Policy

Version 1.5

February 2015

Table of Contents

Revision History

Version	Date	Description
V1.0	2014-9-24	Release
V1.1	2014-10-16	1. Add the additional information for privacy shield. 2. Modify some description to comply with requirement.
V1.2	2014-10-28	Change the first page and description of tail.
V1.3	2014-12-23	1. Modify the description of Product Type. 2. Modify the description of PIN Confidentiality. 3. Correct the range of temperatures monitor. 4. Update the statement of Key Management and Signing Mechanisms
V1.4	2015-01-28	1. Correct the wrong description of Cryptographic Algorithms. 2. Correct some wording for Software Development Guidance.
V1.5	2015-02-05	1. Add more information in section "Software Development Guidance" for reader to understand which details can be obtained from the reference. 2. Correct the 10th doc's name in Reference List.

1 Introduction

This document describes how to use the BEKO 300TR in a secure manner, includes below information,

- Product overview
- Product identification
- Hardware/Software guidance
- Key Management
- PIN Confidentiality
- Decommissioning

Using any unapproved method which not addressed in this document will violate the PCI PTS approval of the device.

2 References

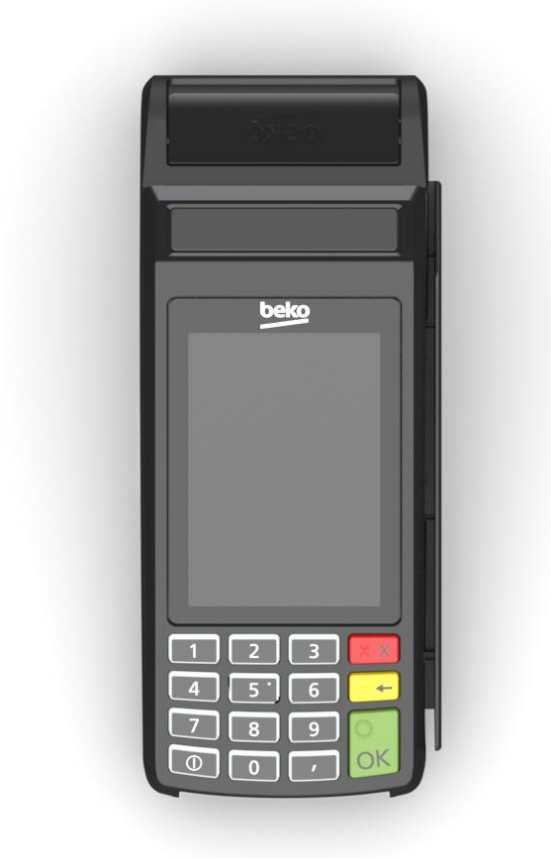
This policy shall be used in conjunction with the following publications.

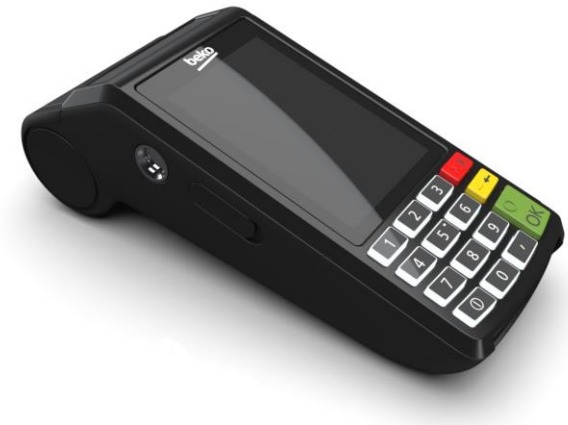
[1] PCI PTS POI Modular Security Requirements Version 4.0 - June 2013
[2] PCI PTS POI Modular Derived Test Requirements Version 4.0 – June 2013
[3] ANS X9.24-1:2009, Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques
[4] X9 TR-31 2010, Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms
[5] ULD CAP Specification
[6] ULD Loader Key Management
[7] ULD Specification
[8] BEKO 300TR Book 2 User Manual
[9] BEKO 300TR Book 4 CTOS API
[10] BEKO 300TR Security Guidance

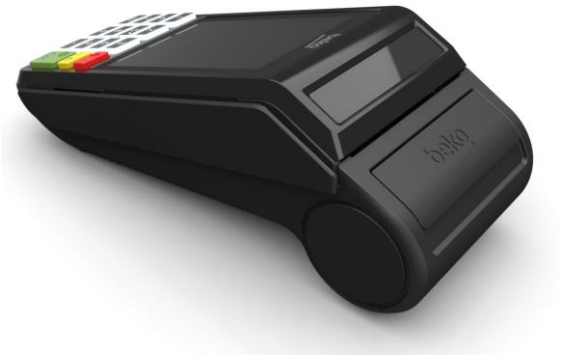
3 Product Overview

3.1 Product Name

The product name is BEKO 300TR. It is visible on the label of device, and should not be modified by any way, or covered by any sticker.



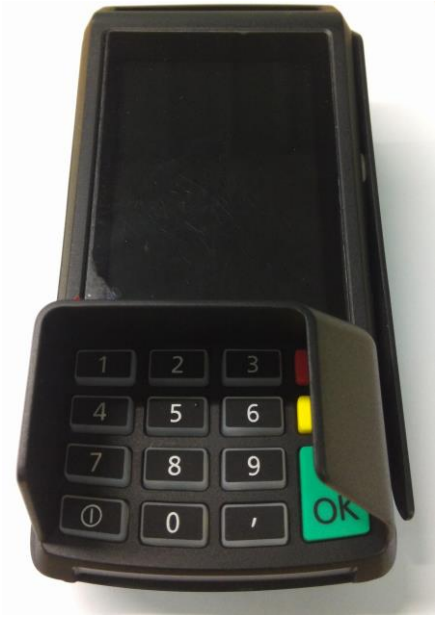




3.2 Product Type

BEKO 300TR is intended to be used as a desktop POS in the attended environment. It is forbidden to use in an unattended environment, use of device in an unattended environment will violate the PCI PTS approval of the device.

For PIN confidentiality, the privacy shield shall be installed on the device as below.



3.3 Product Features

BEKO 300TR provides the features as below,

- LCD (320 * 480 pixel)
- Customer LCD (50 * 8 pixel)
- KBD (15 keys)
- USB
- ICC
- MSR
- Contactless Reader
- Bluetooth

- Ethernet
- Wifi
- GPRS
- Printer

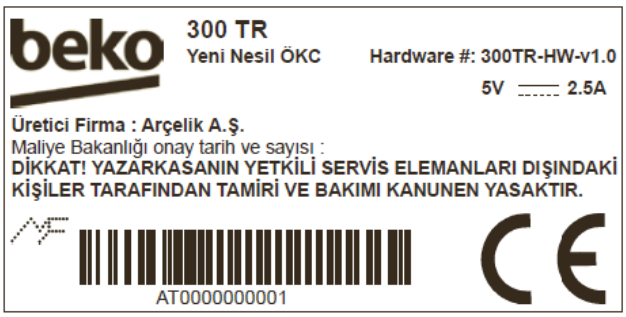
4 Product Identification

4.1 Name

The product name is visible on the label of the device. It should not be modified by the merchant or covered by a sticker.

4.2 Hardware Version

The hardware version is printed on the label which is on the back of device. It is to be notice that the label should not be torn off, covered or altered.



4.3 Firmware Version

The firmware version can be retrieved from System Info Menu by following operations,

- Enter System Menu
- Enter System Info

All the items of firmware are listed here exhaustively, including, boot loader, security, and other non-security-related firmware.

SYSTEM INFO		
BIOS	:	V R x x x x
SULD	:	V R x x x x
LINUXKNL	:	V R x x x x
ROOTFS	:	V R x x x x

5 Product Guidance

5.1 Device Security Inspection

After receiving the device, the acquirer/merchant should visually inspect the items we advised below,

- Inspect the name on the front of device to make sure that no any modification and no any sticker covered.
- Inspect ICC acceptor to make sure that no any untoward obstructions or suspicious objects at the opening.
- Inspect MSR slot to make sure that no any other additional reader or inserted bugs.
- Inspect appearance of device to make sure that no any tamper evidences. It is important checking especially for keypad area.
- Inspect the hardware version from the sicker which is on the back of device.
- Power on the device, check if any tamper warning message is showed on the screen.
- Inspect the firmware version, and check if it runs well.

We strongly recommend periodically inspect the device with above items except for the initial security inspection.

5.2 Installation Guidance

The BEKO 300TR is designed to be portable and does not need installation.

5.2.1 Configuration Setting

The firmware does not use any security sensitive configuration setting.

5.2.2 Default Value Update

When receiving the device from acquirer, it is no any sensitive default value that necessary to be changed before operation.

5.3 Periodic Inspection

The acquirer or merchant shall inspect the device periodically, especially below items,

- Inspect ICC acceptor to make sure that no any untoward obstructions or suspicious objects at the opening.
- Inspect MSR slot to make sure that no any other additional reader or inserted bugs.
- Inspect appearance of device to make sure that no any tamper evidences. It is important checking especially for keypad area.

6 Hardware Security Guidance

6.1 Tamper Response

The device equips protection mechanism for physical tamper attack. Any penetration attempts on the device will trigger the security alarm. The device will switch to inactive mode, and lock itself immediately. In inactive mode, the device will forbid any operations, and show the warning message on the screen. It is to be contributive for acquirer or merchant to differentiate the tampered device easily.

Once the device is locked in tampered status, it has to pass security checking and maintenance before back to normal mode. If acquirer or merchant find any devices are in tamped status, they have to contact the service provider immediately, remove them from service, and kept them for necessary inspection.

6.2 Environment and Operational Conditions

The security of the device is not compromised by altering environmental and operational conditions, includes temperatures and voltages outside the stated ranges.

	Low	High
Temperatures Monitor	-40 ±5 ºC	120 ±5 ºC
Voltages Monitor	2.2V	4.0V

7 Software Security Guidance

7.1 Software Development Guidance

The document [10] is a guidance which provided for the authorized client to ensure the device is used securely, including,

- The requirement for acquirer and software developer.
- The procedural controls to ensure that the applications are properly reviewed, tested and authorized.
- The functions certified by PCI PTS.

The certified functions are outlined as below,

- Key Management System, the secure key loading method, and crypto functions for application.
- Open Protocol, the physical interfaces and communication protocol.
- SRED, the secure method for data exchange.

For more details, please refer to document [10].

7.2 Signing Mechanisms

All the firmware and application are necessary to be signed.

The cryptographic algorithms utilized for signing are listed as below,

- RSA 2048, used for signature verification.
- SHA256, used for calculating hash for data integrity.

For more details, please refer to document [5] [6] [7].

7.3 Patch Procedures

The authenticated user can login to our patch information server to check if any new firmware is released. Once any mandatory patch is released, we will take the initiative in informing the clients. For the updating procedures, please refer to document [8].

7.4 Self-Test

Device will perform the self-test when power on. The items of self-test includes,

- Hardware security status
- Firmware integrity and authenticity

Every 24 hours, device will reboot automatically. Therefore, device can perform self-test periodically by this way.

Once any failures are detected in process of self-test, device will show the warning message, and switch the status to inactive mode. All operations will be forbidden in this status.

8 Key Management

CTOS KMS2 shall be used for key management, using other methods for key management will invalidate the PCI PTS approval of the device.

8.1 Key Management Techniques

The device equips the key management techniques as below,

- Master Key / Session Key, the technique based on a hierarchy of keys. Master Key is directly used to encrypt Session Keys which is unique per transaction. The technique is specified in document [3].
- DUKPT, the technique based on a unique key per transaction, as specified in document [3].

8.2 Cryptographic Algorithms

The device includes the algorithms as below,

- TDES (112 bits and 168 bits)
- AES (192 bits)
- RSA (Signature Verification, 2048 bits)
- SHA256

8.3 Key Type and Usage

The supported transaction key of device lists as below,

- PIN Encryption Key, such keys are used to protect cardholder PIN, and generate cipher-text PIN block.
- Data Encryption Key, such keys are used for data encryption only.
- MAC Key, such keys are used to generate message authentication code.
- Key Block Protection Key, such keys are used to calculate the data key and MAC key for TR31 specified in document [4].
- IPEK (Initial PIN Encryption Key), such keys are used to calculate session keys for each transaction. The technique is specified in document [3].

Device doesn't have any default key at the beginning. Acquirer has to generate and inject all transaction keys before deploying. Each key should be used for specified purpose, and refused to export by any way.

Any violation will invalidate the approval of this device.

8.4 Key Loading Method

The device does not propose manual cryptographic key entry and remote key injection. The key loading device which is complied with PCI PTS requirement shall be placed in a secure environment and used for initial key injection.

The initial keys defined as below,

- KBPK (Key Block Protection Key)

All initial keys shall be loaded into the device by the trustee using the authentic key loading device in secure environment.

The key loading method for application is TR31 (Binding Method) specified in document [4].

8.5 Key Replacement

Any keys should be replaced with a new key value whenever the compromise of the original key is known or suspected, and whenever the time deemed feasible to determine that the key by exhaustive attack elapses.

9 PIN Confidentiality

BEKO 300TR is a desktop device which provided the privacy shield for PIN confidentiality in the transaction.

To avoid disclosing from intended or unintended sight, one of methods is providing the easy-to-understand message or logo for cardholder by payment application, for example, show the message “Prevent from others view when entering PIN” on the screen for cardholder. Such information for cardholders can notify them to take notice of privacy during PIN entry, such as cover the keypad with free hand, or block the possible view by own body.

Additionally, acquirer, administrator, and merchants have to make sure to enter their PIN safely.

10 Decommissioning

If device leave service temporarily, all sensitive data are kept and protected by battery power supply, no any operations for change state of device are needed.

If device is permanently decommissioned from the service, it can be done by disassembling of device to lead it into tampered status, then any operation of device will be forbidden, and all sensitive data will be erased immediately.